Emerging Mobile Payment Technology: Cybersecurity, Disruption and Risk Development

Kaya Kazmirci
CISA, CRISC, CISM, CGEIT, CISSP, Cobit 2019

Kaya Kazmirci

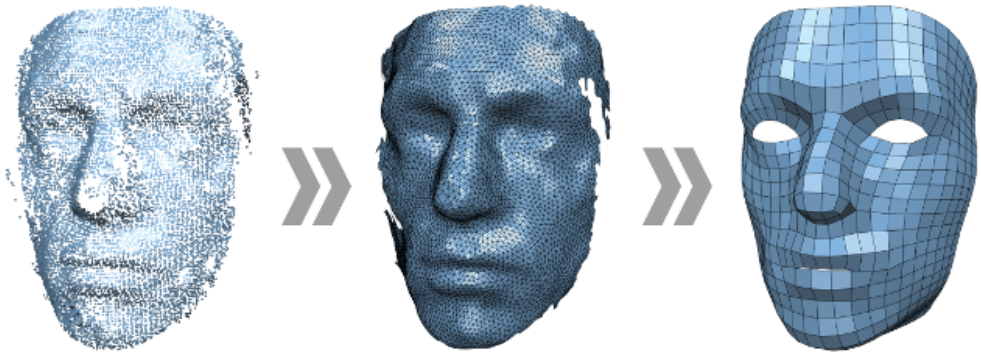
- IT Governance and Cybersecurity, Adjunct Professor, *Bosphorous University of Istanbul*
- Managing Director, Kazmirci Associates
- Internal Audit Director, Mobile Telco
- Head of Sourcing (3 countries), Ericsson
- Audit Senior Manager, EY
- Founder, ISACA Istanbul Chapter (mentoring other chapters in formation)
- Chair and Past Chapter President, Education Committee
- Chair, Cobit 19/CISA Translation Committees
- Regulatory Consultant & Trainer, Cobit Evangelist

Contact Information
Kaya@kayakazmirci.com
Kaya.kazmirci@isaca-istanbul.org
+90532 487 7756

What Do You Want To Learn?

1) Understand the operational details of several emerging technologies including:

- ❑ Quantum Computing
- ❑ AI/ML
- ❑ IoT
- ❑ Image Processing



- ➢ These emerging technologies could significantly disrupt present operational norms as well as introduce improved ways of working.

What Do You Want To Learn?

2) Describe the ways that these emerging technologies might interact with each other and how these interactions impact us.

e.g. IoT and Image Processing will enable enterprises to visually monitor us 24/7, and thus enable a 1984esque police state.

What Do You Want To Learn?

3) Review vulnerable industries including:

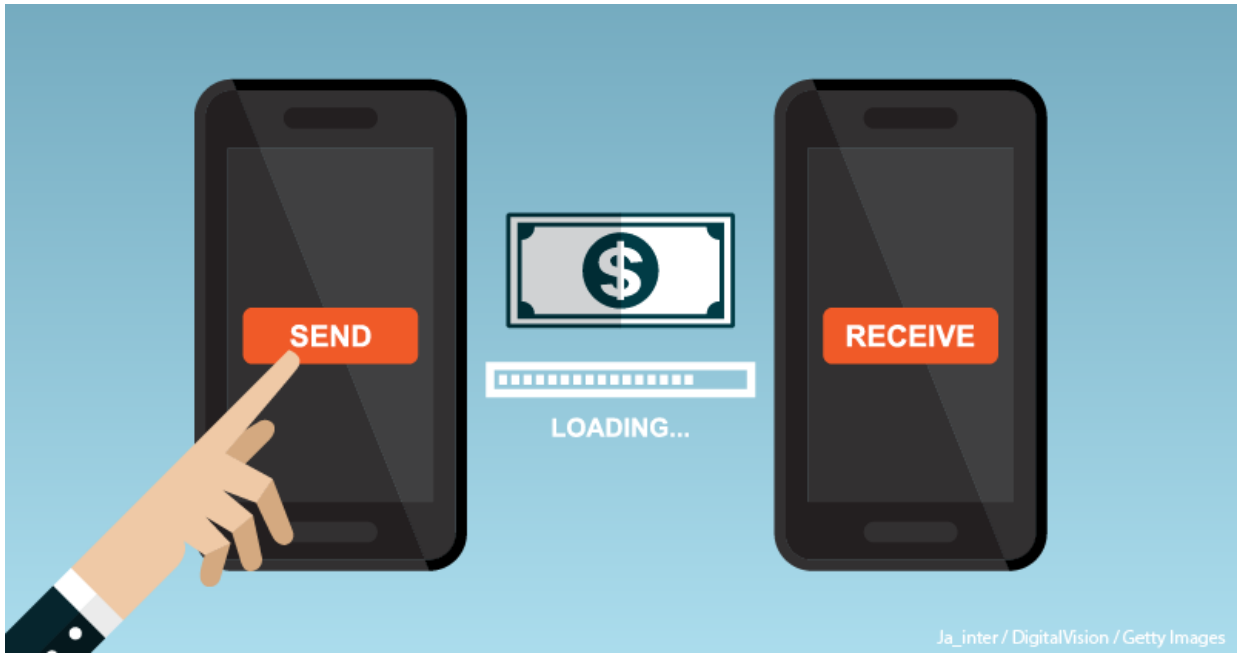
- ❑ Financial services
- ❑ Telecommunications

What Do You Want To Learn?

4) Review opportunities to avoid disruption prone technologies such as present encryption method enabled blockchain applications.

What Do You Want To Learn?

5) Assess governance initiatives that could impact emerging payment technology risk (both disrupting and enhancing)



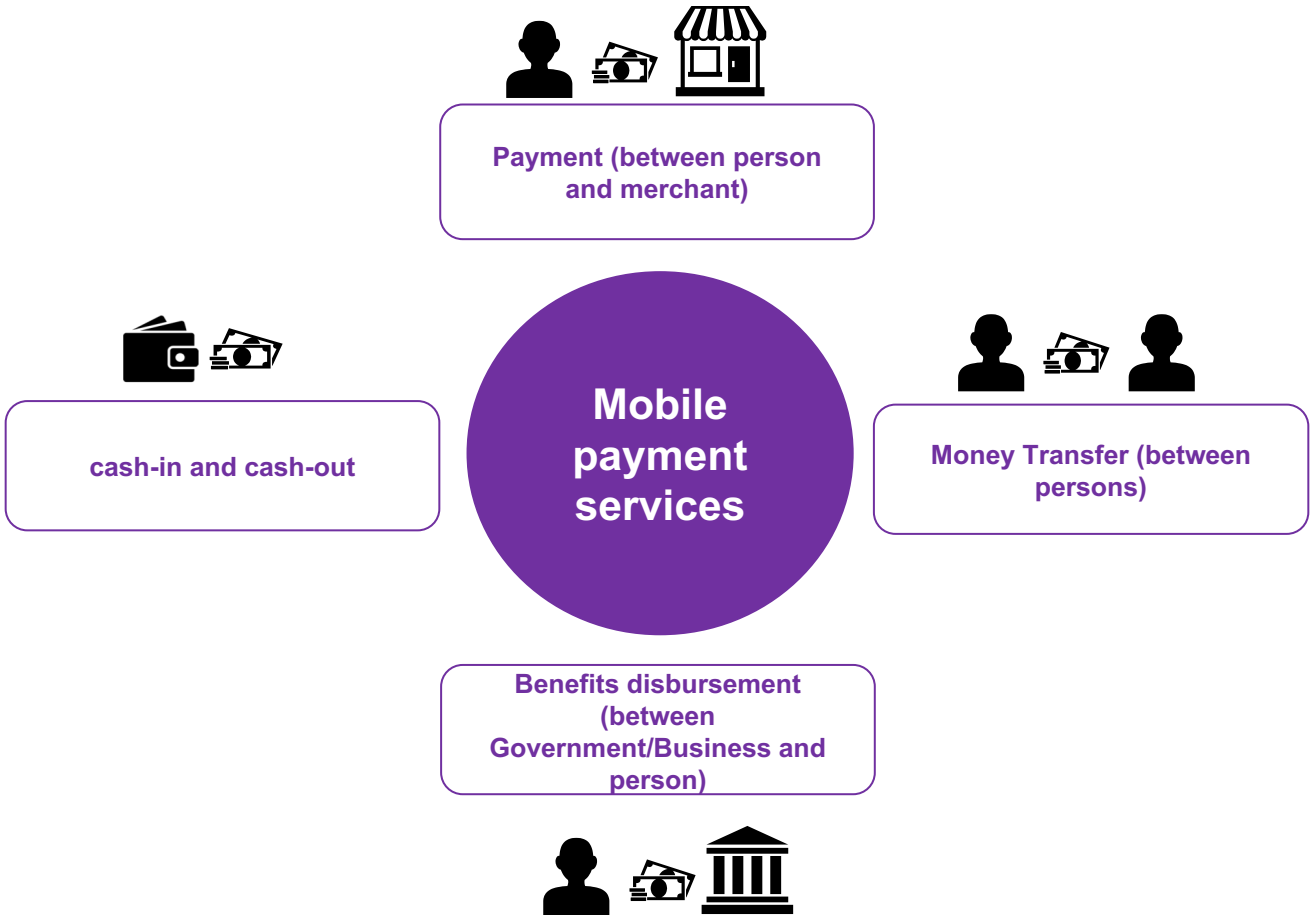
What Do You Really Want To Learn?

- ❑ Is Bitcoin a good investment?
- ❑ How payment tech works
- ❑ How payment tech can fail
- ❑ What do I audit?
- ❑ How can I make it cheaper/better/more secure?
- ❑ Where it is going?
- ❑ Something else?

Who are you?

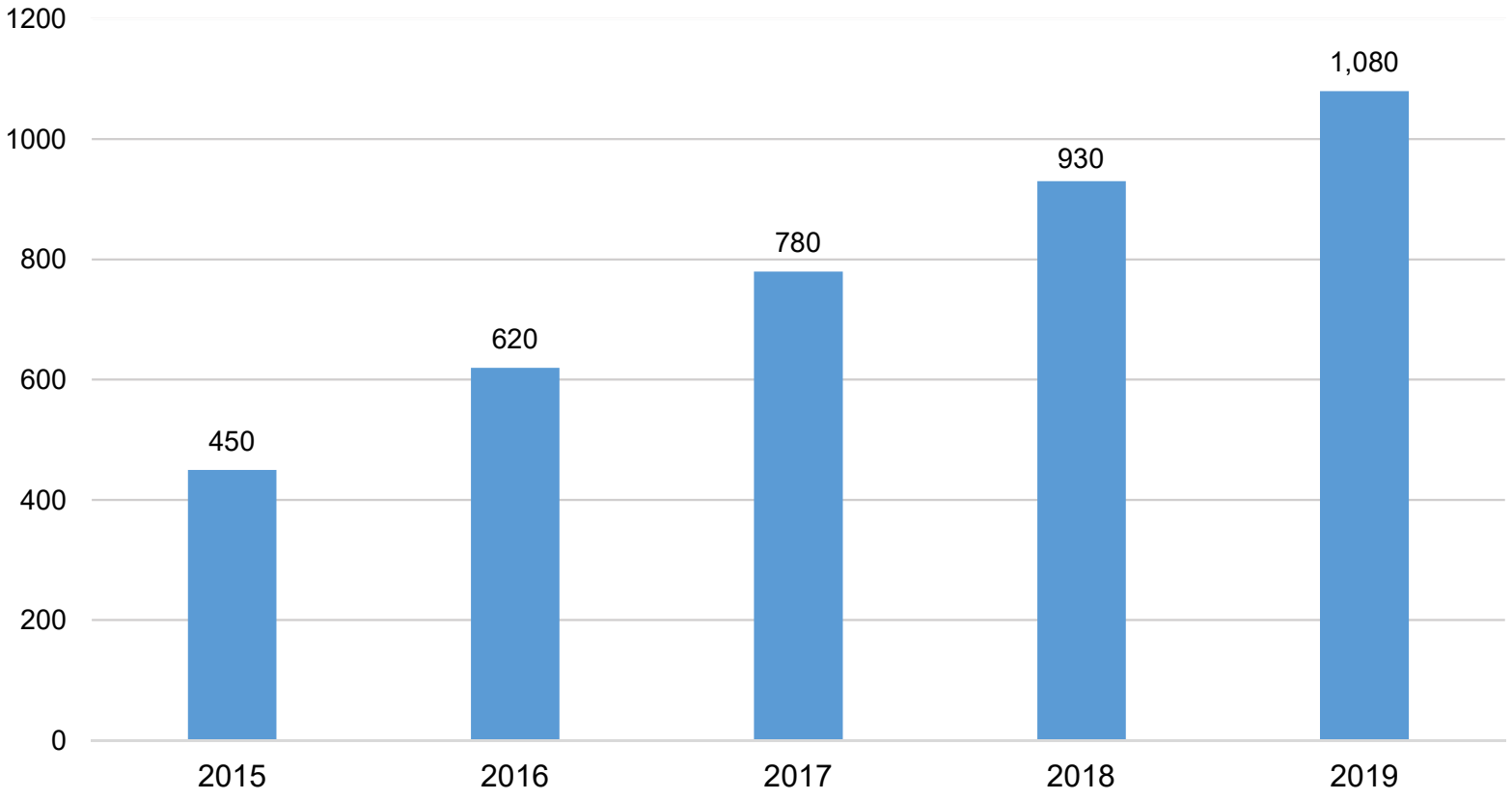
- ❑ Blockchain users
- ❑ CAE
- ❑ Governance Committee Member
- ❑ Operational Audit
- ❑ Business
- ❑ Consultant
- ❑ Others?

What Are Mobile Payments?



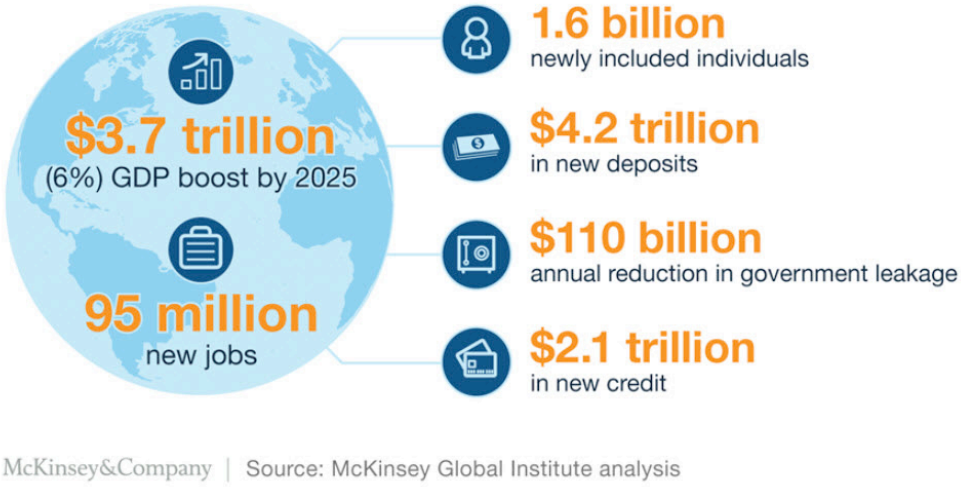
Mobile Payment Growth

Global mobile payment transaction value (USD billion)

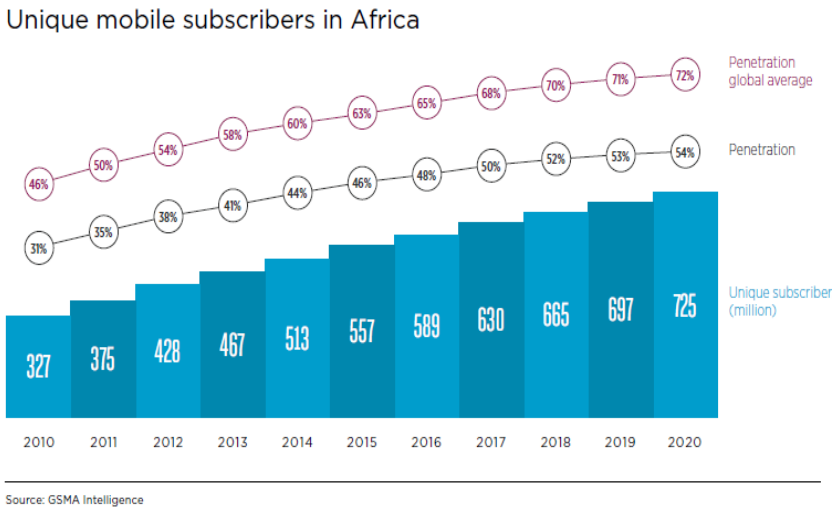


Source: TrendForce

Digital Financial Growth in the Developing World

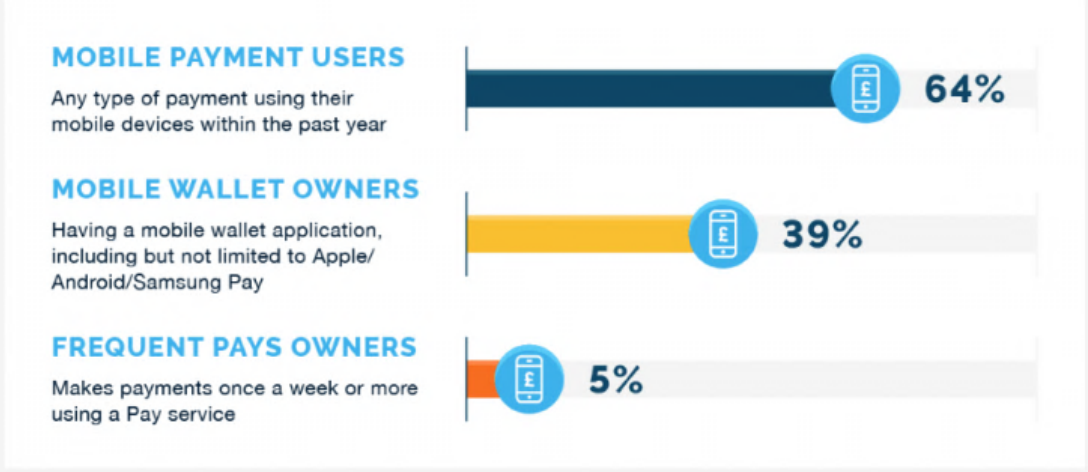


McKinsey&Company | Source: McKinsey Global Institute analysis



Source: GSMA Intelligence

Mobile Payment Uptake



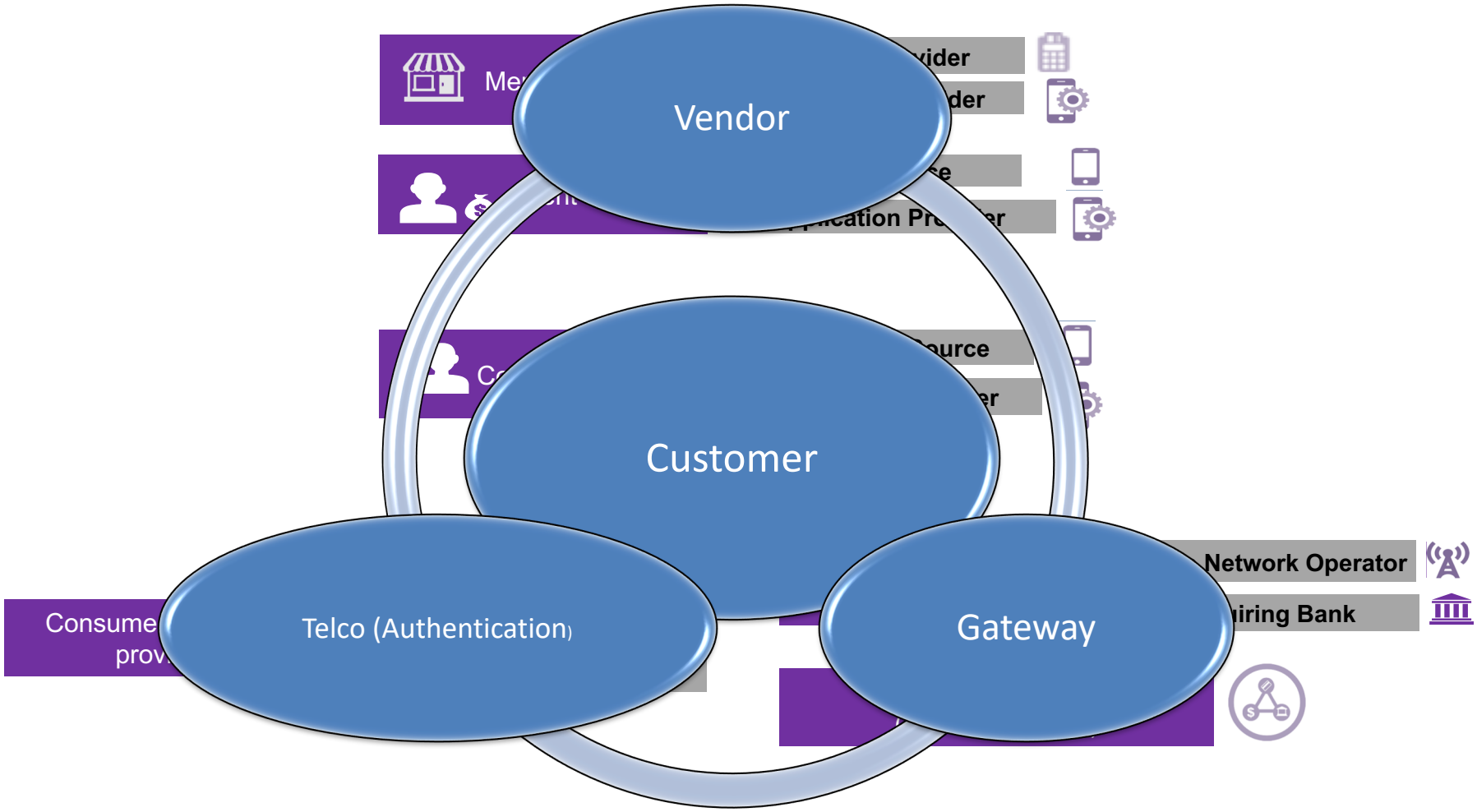
Mobile contributing to economic and social development across the world

Delivering digital inclusion to the still unconnected populations
Mobile internet penetration
2015: 25%
2020: 41%

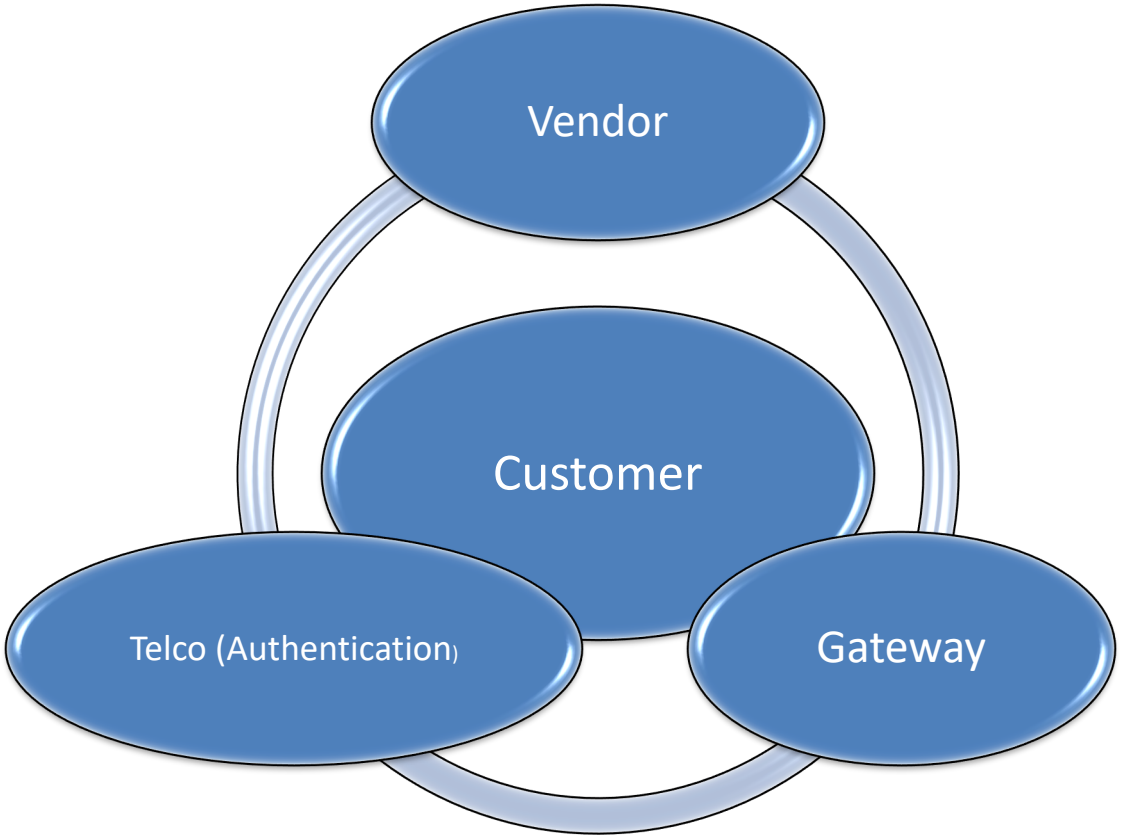
Delivering financial inclusion to the unbanked populations
in 42 countries in Africa
via 157 service providers
as of June 2016

Delivering innovative new services and apps
Number of M2M connections to reach 36m by 2020

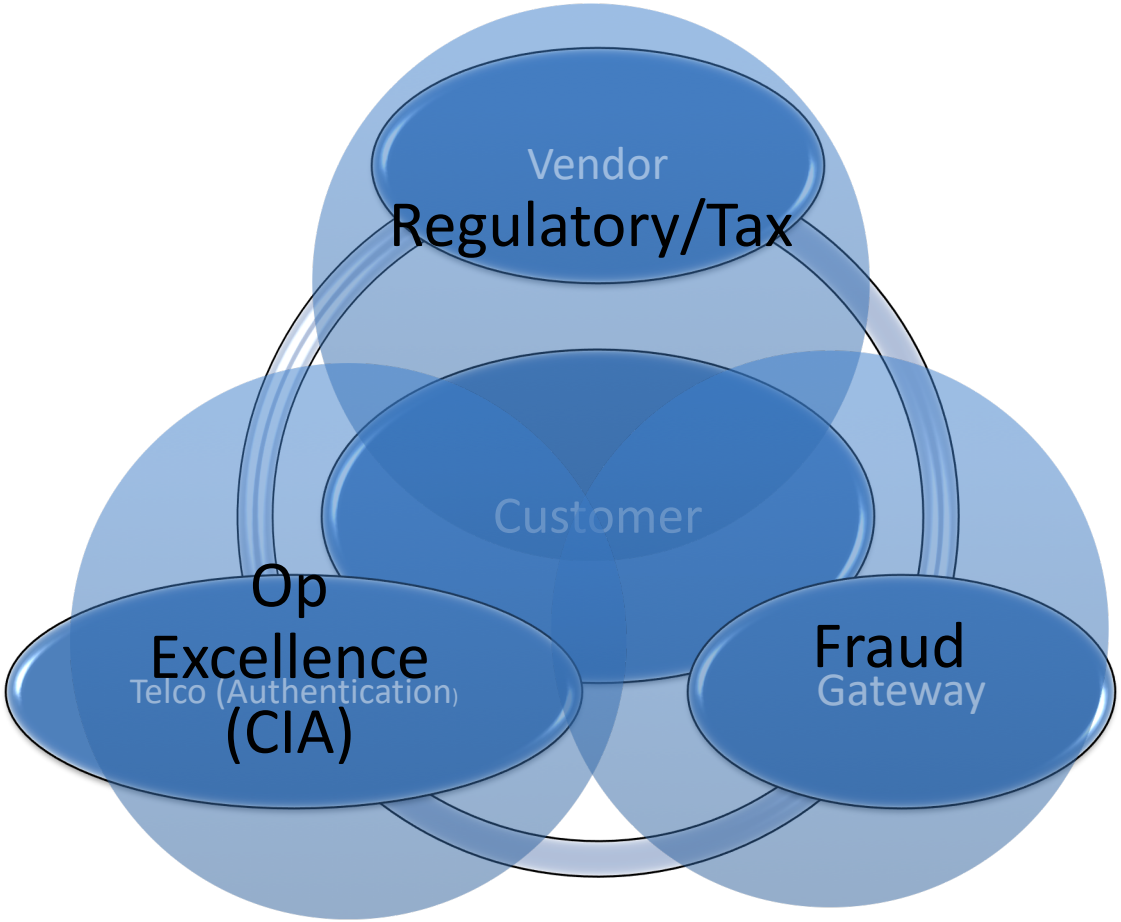
Mobile Payment Ecosystem



Primary Payment Stakeholders



Mobile Payment Risk Areas



What Matters to Vendors?

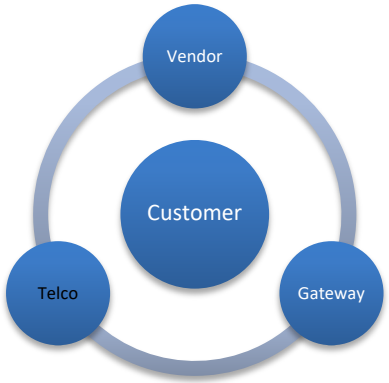
- Prepaid costs: 6%
- Postpaid costs: 7%->3%->1%->0%
- Economies of Scale (Who pays for infrastructure?)
- Who gets paid, how much and when?
- Who carries the risk?
- Public Transport
- Grocery Stores
- Entertainment
- Health Care
- State
- Brick to Click Conversion

What Matters to Telcos?

- Source Authentication
- Network Access Fees
- Point of Sale Cost
  - -Fixed: 3 €/mon
  - -Mobile: 0.3 €/mon
  - -App: ~0 €

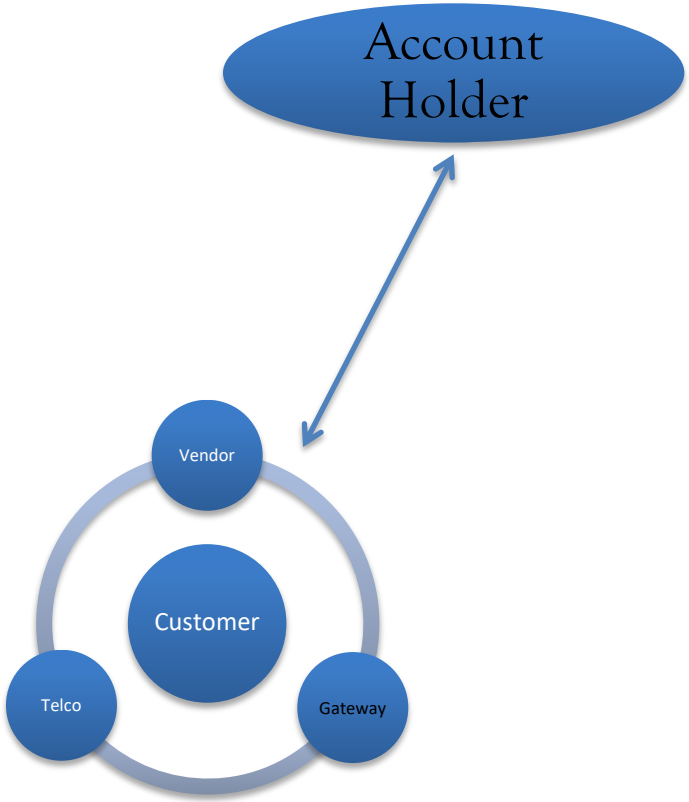
- Fixed to Mobile to App to Bit Pipe
- "fighting gravity"
- Churn Management
- Decreased Customer Aqcuisition Cost

"Trying to get a piece"



What Matters to the Gateway?

- Fees
  - % of Total
  - Transaction
- Account Holder
- Approval/Clearance
- Bank (very fat and scared)
- Telco (?)
- MC, VISA, Amex, Discover, Diner's Club
- PayPal, Google Wallet, Amazon Payments
- Bitcoin (emerging blockchains)

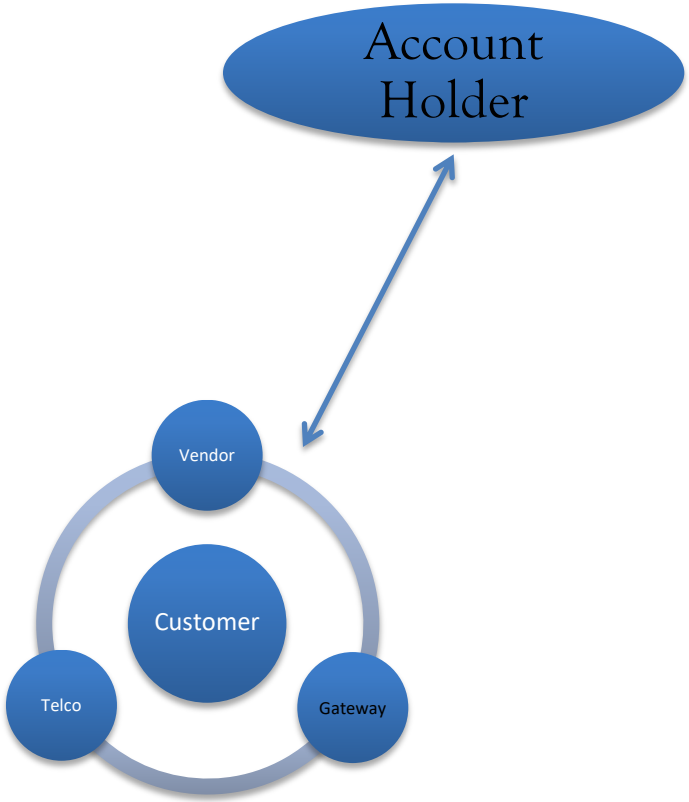


What Matters to the Gateway?

- Fees
  - % of Total
  - Transaction
- Account Holder
- Approval/Clearance
- Bank (very fat and scared)
- Telco (?)
- MC, VISA, Amex, Discover, Diner's Club
- PayPal, Google Wallet, Amazon Payments

DISRUPTS The Gateway!

- Bitcoin (emerging blockchains)



Paypal, Venmo, Applepay, Googlepay and Wanna Be's (Levelup, Square Cash, Android Pay & Qkr)

- Direct customer contact
- App based authentication (low transaction cost)
- International service
- Generally unregulated
- Innovation focused
- Credit Card source

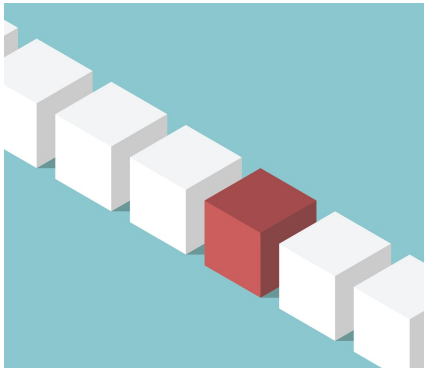
Top 10 Cryptocurrencies

#	Coin	Price	Direct Vol.	Total Vol.	Top Tier Vol.	Market Cap	Chg. 24H
1	Bitcoin BTC	$ 8,007.04	$ 282.16 M	$ 2.62 B	$ 1.14 B	$ 144.09 B	-3.90%
2	Ethereum ETH	$ 174.28	$ 59.81 M	$ 1.19 B	$ 339.83 M	$ 18.85 B	-5.31%
3	Ripple XRP	$ 0.2836	$ 31.07 M	$ 503.36 M	$ 197.17 M	$ 28.36 B	-3.70%
4	EOS EOS	$ 2.893	$ 9.23 M	$ 506.07 M	$ 149.79 M	$ 2.95 B	-7.28%
5	Litecoin LTC	$ 52.54	$ 14.00 M	$ 433.47 M	$ 94.18 M	$ 3.31 B	-5.47%
6	Bitcoin Cash BCH	$ 218.82	$ 27.33 M	$ 230.91 M	$ 75.06 M	$ 3.95 B	-3.26%
7	Binance Coin BNB	$ 17.74	-	$ 88.99 M	$ 65.63 M	$ 2.76 B	-2.72%
8	TRON TRX	$ 0.01497	-	$ 87.32 M	$ 61.36 M	$ 999.21 M	-4.30%
9	Chainlink LINK	$ 2.200	$ 9.33 M	$ 70.18 M	$ 55.07 M	$ 2.20 B	-13.76%
10	Ethereum Classic ETC	$ 4.408	$ 1.81 M	$ 148.35 M	$ 54.90 M	$ 503.86 M	-5.83%

Source: coinmarketcap

Blockchain (Bitcoin is greater than 50% of the Market)

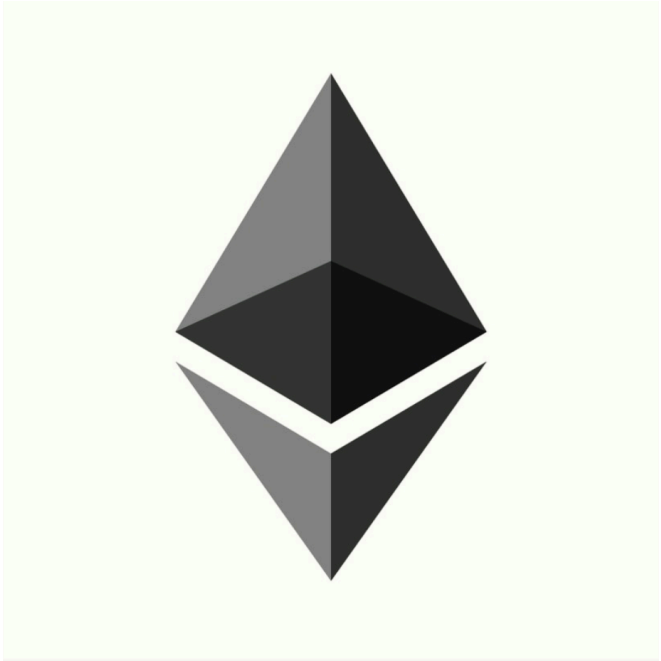
- Distributed ledger
- A Coin is an instrument w/a price (M2M)
- Each Coin in use carries a record of each of its owners
- All transactions are as transparent/opaque as the parties want them to be
- Transactions
  - Close in about 10 minutes
  - Cost based on bid/offer
  - Completed based on Proof of Word (PoW)



- Derivatives can be modeled/executed with a scripting language.
  - Escrow
  - L/C
  - Forward/Swap
  - Micropayments

Ethereum

- Decentralized Virtual Platform
- Uploads and Runs programs
- Conducts transactions
- Executes smart contracts
- Automates traditional processes like:
  - Settlement
  - Accounting
  - Supply chain tracking



Some Other Stakeholders...

Hyperledger

- Linux Foundation initiative
- Open source collaboration
- Distributed ledger and smart contract infrastructure
- Focused on shared record keeping and automated transactions (goods and services)

HYPERLEDGER

Tendermint

- POS consensus mechanism is plug and play
- Every faultless machine records same transactions in the same order
- Application interface enables machines to process every programming language
- Implemented via Cosmos Network
- Initial Coin Offering (ICO) generated 16.8 MUSD in 28 minutes

Libra (Stablecoin)

- *Goal:* Utilize a new digital currency, powered by blockchain
- Expected to launch in 2020
- Facebook running it
- Pegged to a specific commodity price
- They seek to create a stablecoin cryptocurrency centrally administered (POS)
- Who regulates it?

More Stakeholders

- Venture Capitalists
- Blockchain Innovators
- Banks and Financial Services
- Coders and Developers
- NGOs, Academics & Scholars
- Governments
- Legislators
- Regulators
- Law enforcement
- Exchanges
- Miners
- Mining pools
- Token holders

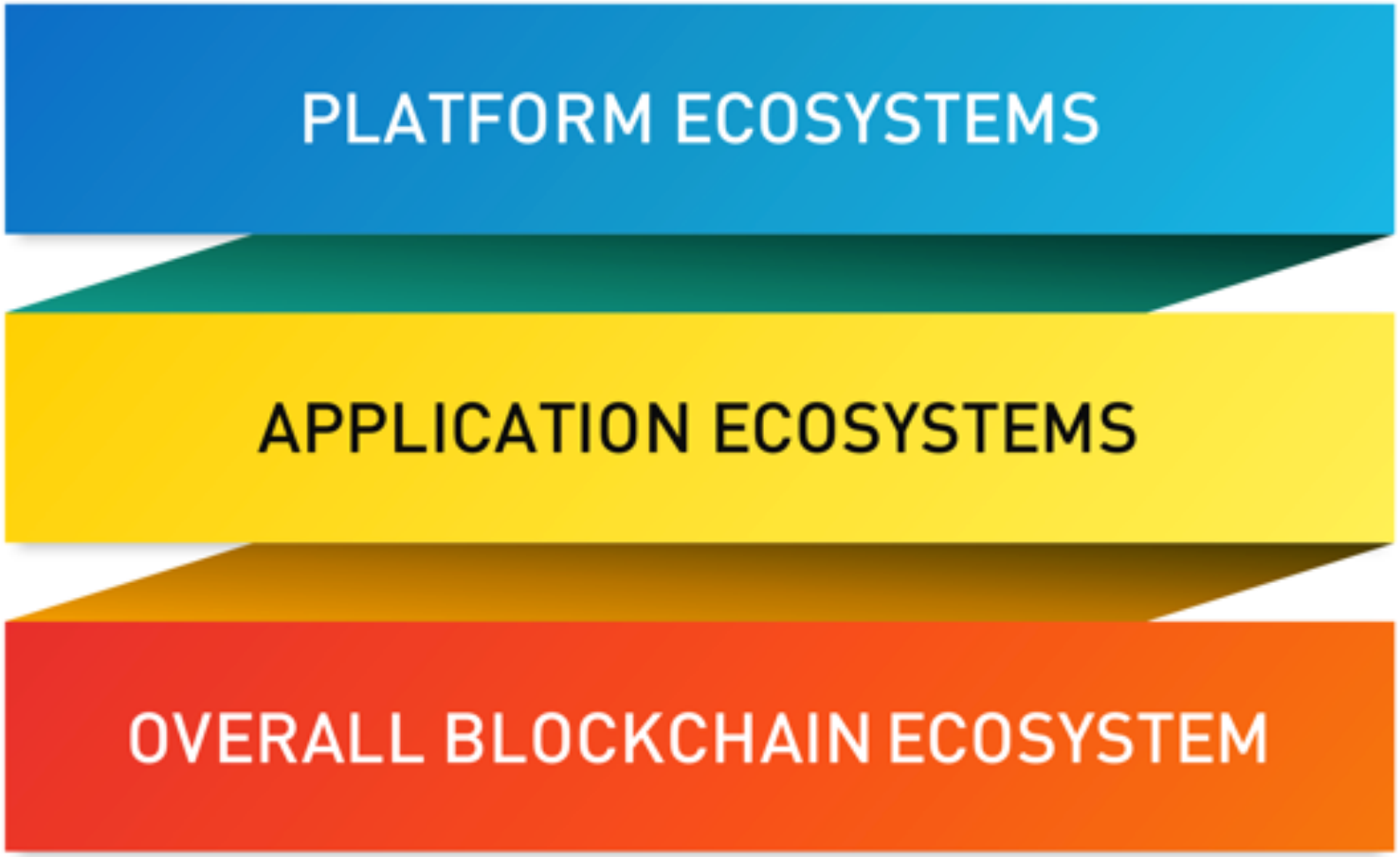
Business Issues

- Payment close time
- Refund right
- Maturity/expiration/Forking
- Notification
- Taxation, AML & KYC
- Right to Audit
- 3rd Party services
- Risk Management
- Local vs International hosting
- Reserve requirements
- Agents
- Fees (micropayment)

IT Issues

- ISMS (privacy, confidentiality, security, integrity, availability)
  - Block size (Network latency vs power/cooling costs)
  - Encryption (key/hash protocol management)
  - Compliance
- Authentication
  - Telco's/states can do it well
  - KYC
- Incident Management
- Logging (data retention requirements)
- Always on
  - RPO and RTO --> 0
  - SDO is resiliant

Governance Areas



Ecosystem Governance Issue?

Platform

Blockchain size

- ❑ Proof of Work (PoW) vs Proof of Stake (PoS)
- ❑ Forking - Bug fixing

Blockchain Overall

- ❑ Quantum computing (Disruptive)
- ❑ Maintain incentives for mass collaboration
- ❑ Failure scenarios?

Application - Proper legal structure for stewardship

- ❑ Premature legislation
- ❑ Business development outpaces regulation
- ❑ Powerful incumbents usurp domain risk (Dictator's learning curve)
- ❑ Synergistically Scale the network

Approaches to Consider...

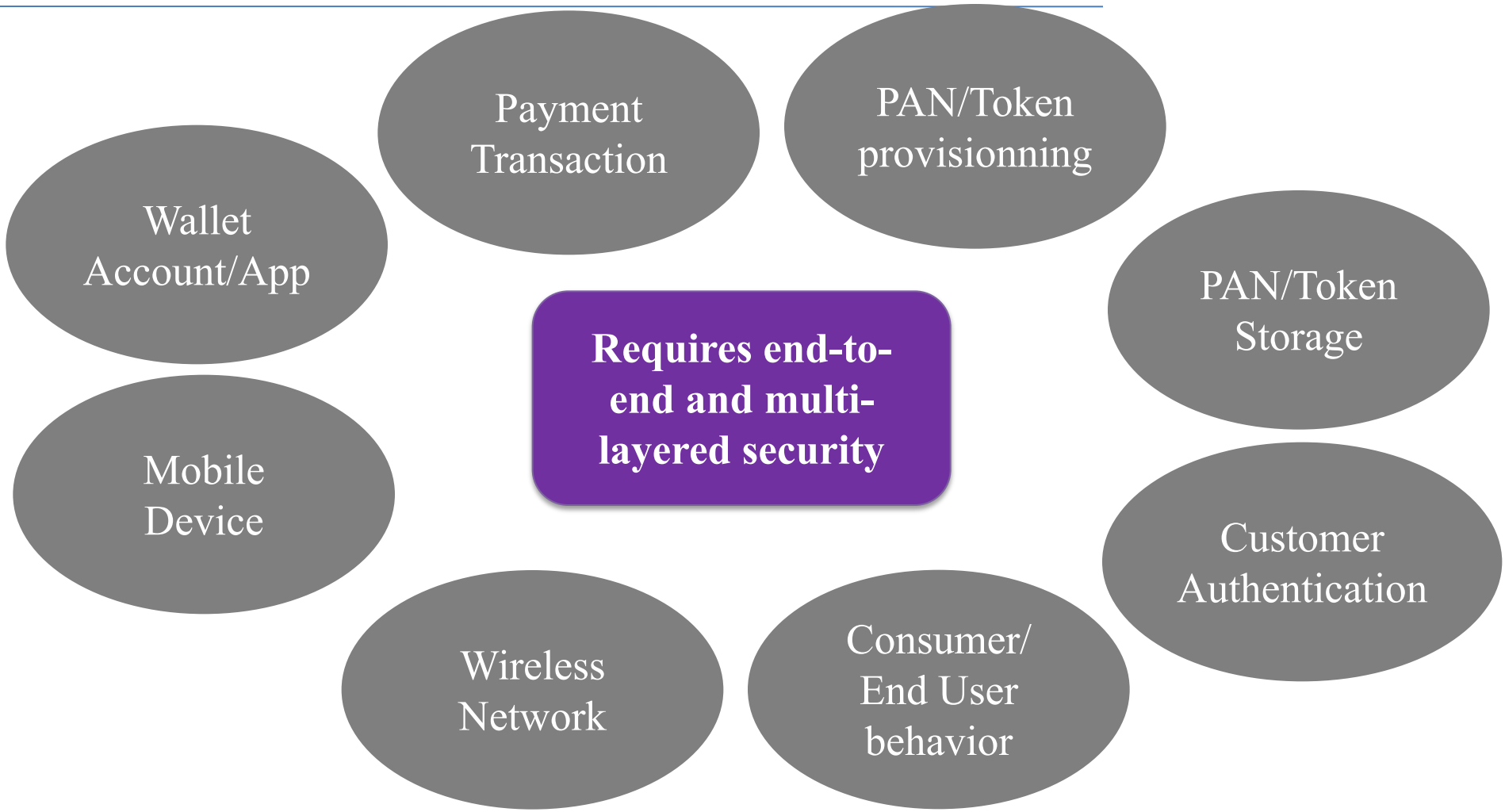
ICANN, IETF or W3C Legislation:

- Jurisdiction,
- Cost to implement/noncompliance
- Post BitLicense, many companies left NYC

Regulated/ Unregulated / Prohibited Services:

- Deposit taking
- Lending
- Payment plan
- Fx
- Stocks/bonds
- Derivatives
- Issueing e-money

Mobile Payment Risks



Main References

- State of the Industry Report on Mobile Money, GSMA, 2018
- The Mobile Economy Africa, GSMA, 2016
- Oversight Issues in Mobile Payments, International Monetary Fund, 2014
- White paper, Is Mobile the Winner in Payment Security?, ISACA, 2016
- Security of Mobile Payments and Digital Wallets, ENISA, 2016
- A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS), ISACA
- The Mobile Money Revolution: Part 1: NFC Mobile Payments, ITU-T Technology Watch Report, 2013
- White Paper, Mobile Payments: Risk, Security and Assurance Issues, ISACA, 2011 .

Acknowledgements

Thank you!

Coşkun Şahin

Salah Eddine Mahrach, CISA, CRISC

Asmae El Morabit, CEH

Derin Arduman

World Economic Forum

ISACA

Appendix 1-Detailed Mobile Risks and Countermeasures

Mobile Payment Risks

Security Measures

- ❑ Security awareness, education and communication.
- ❑ Do not use public Wi-Fi hotspots for mobile wallet payments.
- ❑ Distinguish real and fake website and access point, only use real one.
- ❑ Keep OS up to date and don't use untrusted phone.

Mobile Users Threats

- ❑ Phishing attacks
- ❑ Social engineering
- ❑ Unintentional installation of rogue and malware applications
- ❑ Mobile Operating System Access Permissions

Vulnerabilities

- ❑ Lack of user's due carefulness of validating content in emails, messages, SMS being truthful before selecting URLs, downloading attachments.
- ❑ Use public Wi-Fi connections for mobile payments.
- ❑ Use of fake access point with same network.
- ❑ Use of fake websites.
- ❑ Missing minimum security hygiene rules.
- ❑ To install non-trusted applications and files on device.

Mobile Payment Risks

Mobile Devices Threats

Security Measures

- ❑ Remote device lock and Remote data wipe.
- ❑ PIN lock and Strong PINs.
- ❑ User to device biometrics authentication factors safely.
- ❑ Keep OS up to date.
- ❑ Keep default security controls & measures on device. Secured Biometric validation data.

Mobile Users Threats

- ❑ Unauthorized access of lost or stolen mobile device
- ❑ Data interception via installation of malware
- ❑ Mobile as a target
- ❑ Implementation Issues

Vulnerabilities

- ❑ No PIN lock set or PINs set to weak PINs.
- ❑ No remote devices lock set and no remote data wipe set.
- ❑ Not up-to-date OS to connect and use untrusted device.

Mobile Payment Risks

Mobile Applications Threats

Security Measures

- ❑ Adopt secure coding practices and secure code reviews manual and automated via tools.
- ❑ Source code complication an untrusted code detection.
- ❑ Anti-debug and Integrity source code protections.
- ❑ White-box cryptography.
- ❑ Secure application provisioning through trusted application stores.
- ❑ Takedown rogue applications from unauthorized application stores.

Mobile Users Threats

- ❑ Reverse engineering
- ❑ Tampering with the mobile payment application and the use of rookits
- ❑ Mobile Operating System Access Permissions

Vulnerabilities

- ❑ Hardcoded secrets as private keys.
- ❑ Missing to disable code debugging routines.
- ❑ Unsigned production binaries.
- ❑ Credit card provisioning weaknesses like stolen credit cards to affect sensitive data.
- ❑ Weaknesses in biometric identification for initial authorization of transactions.
- ❑ S/W vulnerabilities and weaknesses in third party applications that provide access to mobile wallets.
- ❑ Weaknesses in payment authorization provisioning with mobile paired smartwatch device.
- ❑ Credit/debit card not stored encrypted in Secure Element or processed in Trusted Execution Environment.
- ❑ Weak PINs exposing them to brute force attacks.
- ❑ Insecure communication channels with Point of Sale (POS) contactless terminals.
- ❑ Insecure tokens used in Magnetic Secure Transmission (MST) connections.
- ❑ Poor signal strength for MST processing.

Mobile Payment Risks

Merchants Threats

Security Measures

- ❑ Change default passwords on POS systems and keep POS software up to date.
- ❑ Deploy and confiUse SSL between POS connection point (POI to POS).
- ❑ gure firewalls.
- ❑ Restrict POI and POS access to authorized users.

Mobile Users Threats

- ❑ Uploading malware (POS) on the POS contactless payment terminal
- ❑ Man-,n-the-Middle (MiTM) attacks against the POS contactless terminal and POS server connections
- ❑ Relay attacks against NFC enabled POS contactless terminal

Vulnerabilities

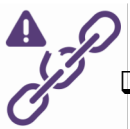
- ❑ Use of default password to access POS terminals available online.
- ❑ POS and POI security misconfigurations and security hygiene such as keeping software up to date, patching systems, etc.
- ❑ Insecure connections between POI and POS
- ❑ Insecure access to LAN and to POS systems
- ❑ Lack of enforcement of minimum privileges for POI and POS access

Mobile Payment Risks

Payment Service Providers Threats

Security Measures

- ❑ Secure by-default design.
- ❑ Vulnerability testing
- ❑ Patching of POI terminal (card machines) H/W and S/W.
- ❑ Fix S/W vulnerabilities in POI.
- ❑ POI and payment gateways hosted at the payment service providers.
- ❑ Enforce secure point to point connections between merchant POS and PSP and between PSP and acquirers.



Mobile Users Threats

- ❑ Compromise of S/W running on contactless terminals
- ❑ Compromise of Payment Gateways
- ❑ Compromise of S/W installed on POS Servers
- ❑ Data connectivity compromise

Vulnerabilities

- ❑ Design flaws and un-patched S/W vulnerabilities in POI terminal/credit card machines and POS systems and payment gateways to/from acquirers.
- ❑ Insecure point to point connections between merchant POS server and PSP and between PSP and acquirers.

Mobile Payment Risks

Acquirers Threats

Security Measures

- ❑ Enforce high security standard measures for payment processing systems and second factor authentication (2FA) for user authentication/access.
- ❑ Enforce minimum privileges for user access.
- ❑ Deploy malware detection, data leakage and fraud prevention.
- ❑ Secure internal point to point connections with SSL/mutual authentication.
- ❑ Require digital signatures to sign and verify payment authorizations from issuer.

Mobile Users Threats

- ❑ Payment processing systems compromise
- ❑ Installation of malware/RAT for Advanced Persistent Threats (APTs):
- ❑ Installation of rootkits
- ❑ Data connectivity (external from acquirer to issuer and internal among servers) compromise
- ❑ Repudiation of mobile payment authorization

Vulnerabilities

- ❑ Un-authorized access to payment processing systems/applications and weaknesses in enforcement of internal security controls and measures to access these systems.
- ❑ Non-effective malware detection, data outflow detection/prevention and fraud detection/prevention.
- ❑ Insecure external and internal point to point system connections.
- ❑ Weak server to server authentication among internal systems.
- ❑ Gaps in non-repudiation controls for processing authorizations such as out of band verification/confirmation of suspicious transactions and digital signing of transactions.

Mobile Payment Risks

Payment Network Providers Threats

Security Measures

- ❑ Secure configuration and hardening of critical servers.
- ❑ Secure key storage in hardware encrypted security modules.
- ❑ Dual controls and strong authentication 2FA to access the token vault.
- ❑ Enforcement of End to End encryption for protecting cardholder data in transit to issuer.
- ❑ Anti-DOS measures are application and network layer to protect token services.

Mobile Users Threats

- ❑ Compromise Token Services
- ❑ Compromise Token services provider servers
- ❑ Denial of Payment settlement services
- ❑ Data connectivity compromise
- ❑ Device and mobile network reliability

Vulnerabilities

- ❑ Misconfiguration of servers providing tokenization services by Non-secure key storage.
- ❑ Insecure user access to the token vault.
- ❑ Insecure connections to/from acquirers and issuers.
- ❑ Weaknesses in protection of Denial of Service (DOS) attacks against TSP service.

Mobile Payment Risks

Card Issuers Threats

Security Measures

- ❑ Enforce strong multi-factor authentication for access to critical systems where credit cardholder data is being stored.
- ❑ Enforce minimum privileges for users that have access to internal critical systems used for verify cardholder data and authorize payments based upon specific business rules.
- ❑ Deploy malware detection and prevention, suspicious activity detection rules based upon aggregated log analysis.
- ❑ Configure fraud detection and prevention systems and enforce fraud management rules for mobile payment transactions.

Mobile Users Threats

- ❑ Credit card Enrolment
- ❑ Payment authorization process compromise
- ❑ Confidential cardholder data compromise through malware/APT
- ❑ Payment fraud
- ❑ Token services data compromise

Vulnerabilities

- ❑ Weaknesses in enforcing strong authentication for access to critical systems and databases where cardholder data is stored for validation and payment authorization to acquirer.
- ❑ Non-effective malware detection and prevention measures.
- ❑ Misconfiguration of fraud detection systems including rules such as positive payment checks, max limit amount per transaction, daily limits, velocity, tagging.

Mobile Payment Risks

Mobile Payment Applications Providers (Servers & Cloud Services)

Threats

- ❑ Compromise of cardholder's sensitive data
- ❑ Compromise of the user profile managed in the cloud
- ❑ Token service data compromise
- ❑ DDoS attacks
- ❑ Enrolment of stolen credit card data entry
- ❑ Accountability for payment transactions
- ❑ Transaction errors
- ❑ Lack of transaction record and documentation
- ❑ Ambiguity of the transaction
- ❑ Third party trust
- ❑ Privacy issues

Vulnerabilities

- ❑ Weaknesses and vulnerabilities on digital wallet servers and applications hosted at the mobile payment application provider.
- ❑ Absence of malware detection and prevention on critical servers that provide access servers where cardholder data and user profiles are stored.
- ❑ Gaps in deployment of 2FA to access servers and maker/checker controls.
- ❑ Absence of fraud detection and prevention for use of stolen credit card holder for enrolment in mobile payment applications.
- ❑ Weaknesses in anti-DoS measures to prevent DoS against digital wallet and account profile services hosted in data centers and cloud services.

Mobile Payment Risks

Mobile Payment Applications Providers (Servers & Cloud Services)

Security Measures

- ❑ Enforce information security policies and processes requiring identification and remediation of vulnerabilities in servers and applications.
- ❑ Deploy malware detection and prevention measures. Enforce 2FA for internal user's access to critical servers such as digital wallet services where cardholder data and user profile information is stored.
- ❑ Enforce user entitlements and minimum privileges.
- ❑ Deploy fraud detection and prevention for high risk functions such as change of account profile, credit card enrolment and payment transactions.
- ❑ Deploy anti-DoS measures for critical servers hosted in data centers and in the cloud.

Appendix 2 – How Mobile Payment Systems Work

Mobile Payment Types

There are payment services based on **text messages** sent by the payer through a mobile device. The payer has to indicate the beneficiary and the amount, which is directly charged to the phone bill. This service is not restricted to smartphones, and is also available on traditional mobile phones, thus contributing to a potentially wider use of mobile payment services.

Direct mobile billing services (also called direct to bill) allow customers to make payments (such as utilities) or credit transfers via their mobile phone account balance without the use of a bank account, a credit card or a financial PSP. Once the user has signed up for the service, she/he is allowed to add money to the network account (using cash or by credit transfer). The user is then authorized to transfer money to other users through the mobile phone menu, using PIN-secured SMS text messages. Money can then be withdrawn from the mobile phone account, after it is confirmed that sufficient funds are available in the user's account. Purchases made using direct mobile billing are charged directly to the user's mobile phone billing account.

Mobile Payment Types

Several **mobile applications for payment** services have been recently developed by financial institutions, telecommunications operators and merchants. Those apps allow customers to pay for goods and services directly from their smartphones or other mobile devices, or to make person-to-person payments. After installing the app, the users have to register and define the authentication credentials.

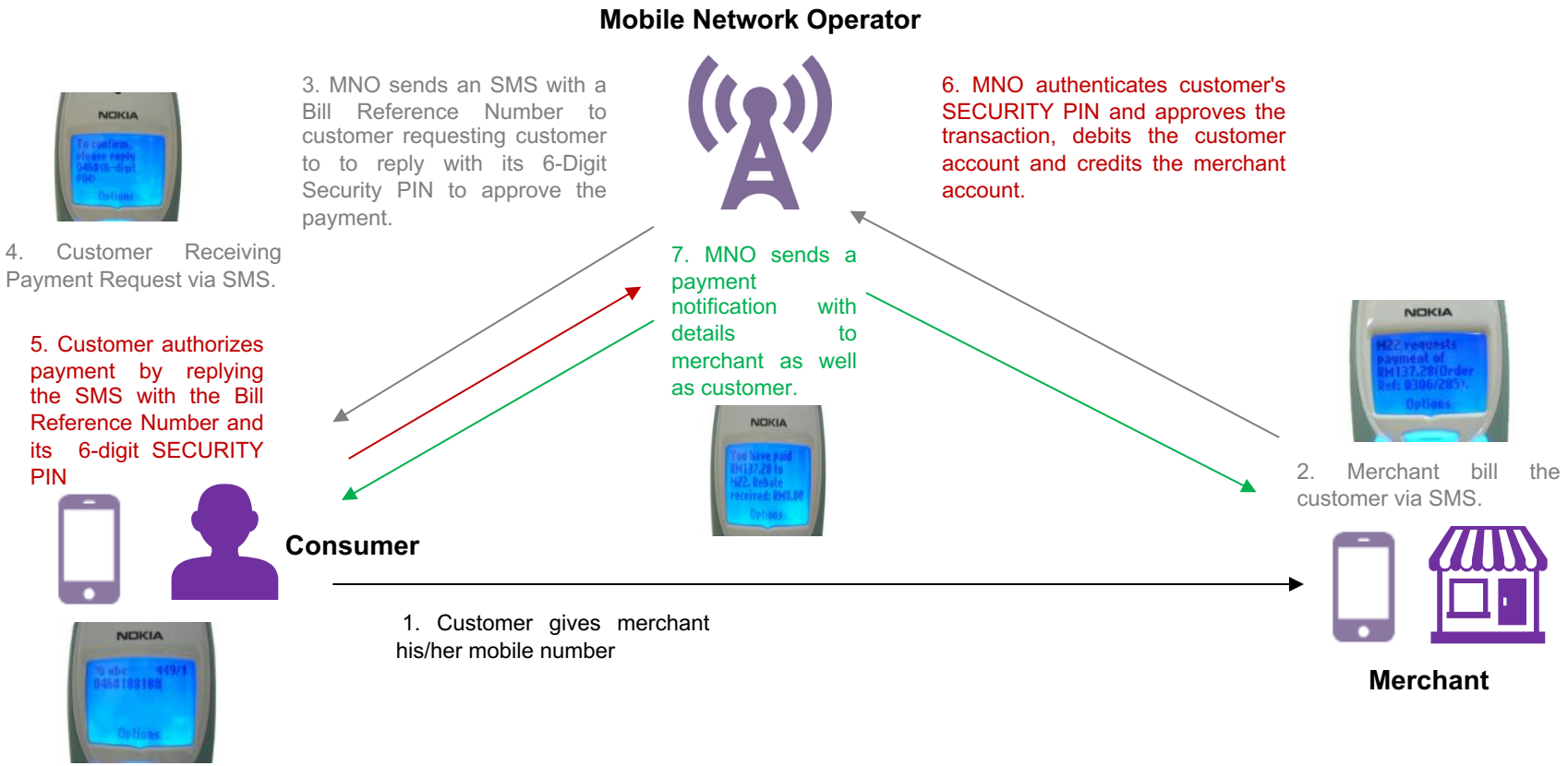
These apps can directly receive payment orders from merchants, requiring users to confirm the order via the app; or they can generate specific codes (including bar codes to be read by bar code scanners, as available, for example, in Austria) to be used by the customer to authorize the payment. With these services, card or account data are usually not transmitted at the POS.

Mobile wallets are a set of procedures agreed between a wallet provider and a consumer to use an NFC-enabled mobile phone as a proximity device to initiate payments using linked payment cards or accounts. As with online wallets, the user can associate a payment card or account, or upload money onto the account by using a card, a credit transfer or cash. Payments are allowed after the user's identity is confirmed (by entering a username and password), and the amounts are directly debited on the user's wallet account. The operations may be ordered through the app buttons or via a contactless solution. This service may be incorporated in banking tools made available to the consumers by their deposit and credit institutions, or offered by a third party.

Mobile Payments in Motion

SMS Transaction

A Customer choose to pay for the goods and services from a merchant using its MNO's account.

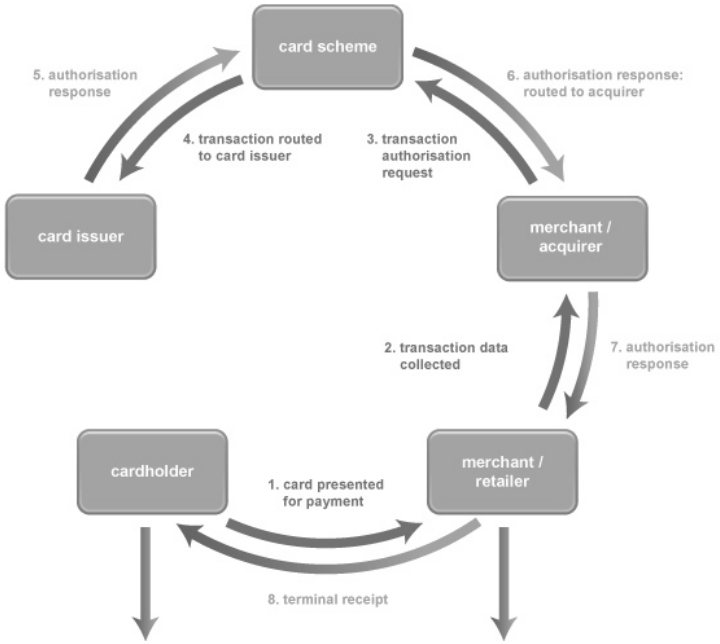


Mobile Payments in Motion

Contactless Mobile Payments

Contactless Mobile Payments that are processed through credit and debit card networks do not change the fundamental design of the system that is already set up for traditional card based payments.

In order to conduct a traditional card based payment transaction typically the cardholder initiates the transaction by transmitting payment authorization data, including the primary account number **(PAN)** to the merchant such as by swiping the card at a point of sale (POS) terminal or by inserting the EMV chip card at the POS terminal. The merchant then relays the information to the acquirer bank (the merchant bank) and then the card network relays this to the bank issuer for the payment to be authorised.



The exact same process is replicated when performed via a mobile device and contactless POS terminal, with the sole difference that the card number **(PAN)** and the **CVC (card verification code)** are typically substituted with what are called tokens instead of the actual PAN and CVC. The reason this is performed is to prevent the actual card number being sent over the wire and subsequently stored in intermediary servers.

Mobile Payments in Motion

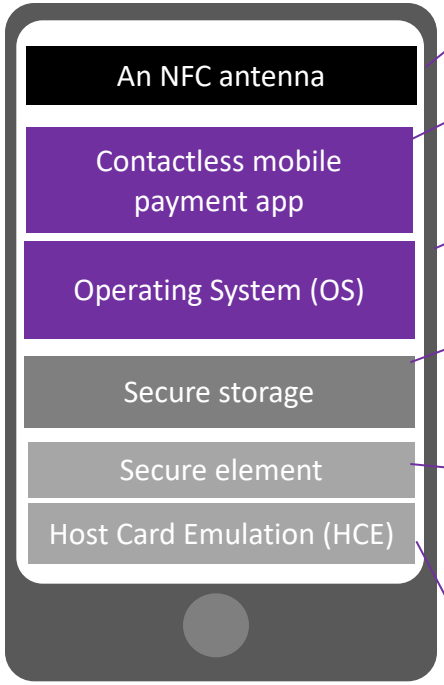
Contactless Mobile Payments Core Concepts

- **PAN:** a unique identifier printed on the front of the card by the issuing bank. Referred to as the *Primary Account Number* , it links the card to the customer's bank account.
- **Expiration Date:** printed or embossed on the front of the card. The expiry date and the PAN constitute the minimum set of card authentication data.
- **CVC/CVV :** stands for *Card Verification Code* or *Card Verification Value* a 3-digit number printed on the reverse side of the card. It is meant to be known only to the person possessing the card. It should not be stored electronically anywhere in the payment ecosystem.

Mobile Payments in Motion

Contactless Mobile Payments Core Concepts

To perform Contactless mobile payments (CMP), a mobile device needs some hardware and software components



The NFC antenna facilitates communication between the CMP app and the retailer's POS terminal.

These apps provide the user interface for CMP services, and facilitate the storage and transmission of payment information.

This enables the mobile device to function, and handles the processing of apps loaded onto it.

It is key to the security of CMPs that payment data can be stored securely, either on the mobile device itself or remotely, within the systems of the app provider

This is a chip used to store sensitive data on a mobile device. The secure element may be embedded in the device (e.g. for Samsung Pay and Apple Pay) or the SIM card (e.g. for the recently closed Vodafone Pay). The secure element stores the tokens representing the consumer's card details registered with the CMP app. It also holds dynamic cryptograms that accompany the tokens to verify them as having come from the consumer's device.

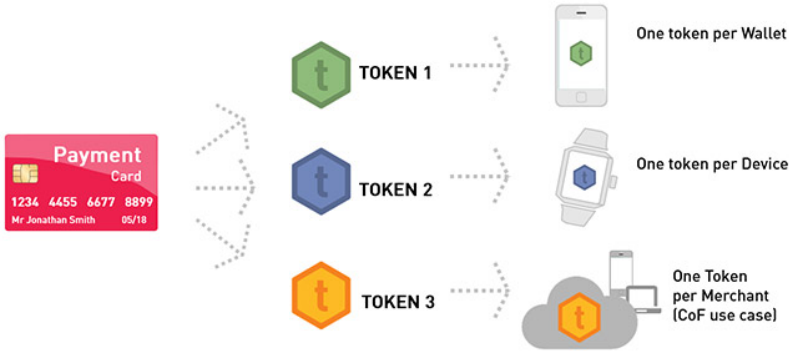
Under this configuration, the CMP app supplier stores the sensitive information (i.e. tokens and cryptograms) remotely on secure servers in host or 'cloud' databases (e.g. for Google Pay). The CMP app uses the mobile device's data connection to the internet to access this information and draw it down onto the device as needed

Mobile Payments in Motion

Contactless Mobile Payments Core Concepts

Tokenization

Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a —token. It is only the token data which is then stored in the mobile device – protecting the real card number from misuse.



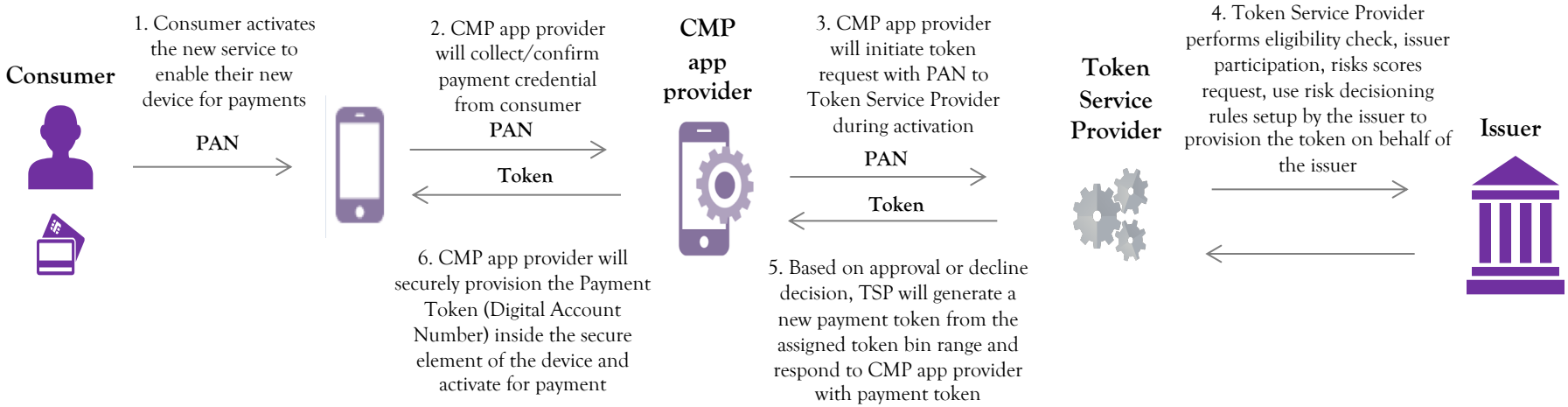
PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

PCI DSS Tokenization Guidelines, Selected Examples of Token Formats

Mobile Payments in Motion

Contactless Mobile Payments Core Concepts

The act of enrolling a payment card for use with a CMP app on a mobile device is known as 'provisioning'. Tokenisation occurs during the card-provisioning process. Consumers enroll their cards with a CMP app by entering their PAN, security code and other information requested by the app. The CMP app provider then requests a token from the Token service provider (TSP). The TSP forwards the request to the card issuer for approval. If that approval is given, the TSP creates a token to replace the PAN and the token is then used in CMP transactions. The TSP stores a list of the tokens and their corresponding PANs in its 'token vault'.



Mobile Payments in Motion

Contactless Mobile Payments Core Concepts

Payment Transaction using Payment Tokens at Point of Sale (NFC)

Mobile payments that are processed through credit and debit card networks do not change the fundamental design of the system that is already set up for traditional card based card payments.
A token PAN can be used just like payment credentials in the existing payment acceptance network and is totally transparent for the consumer when they make a purchase.